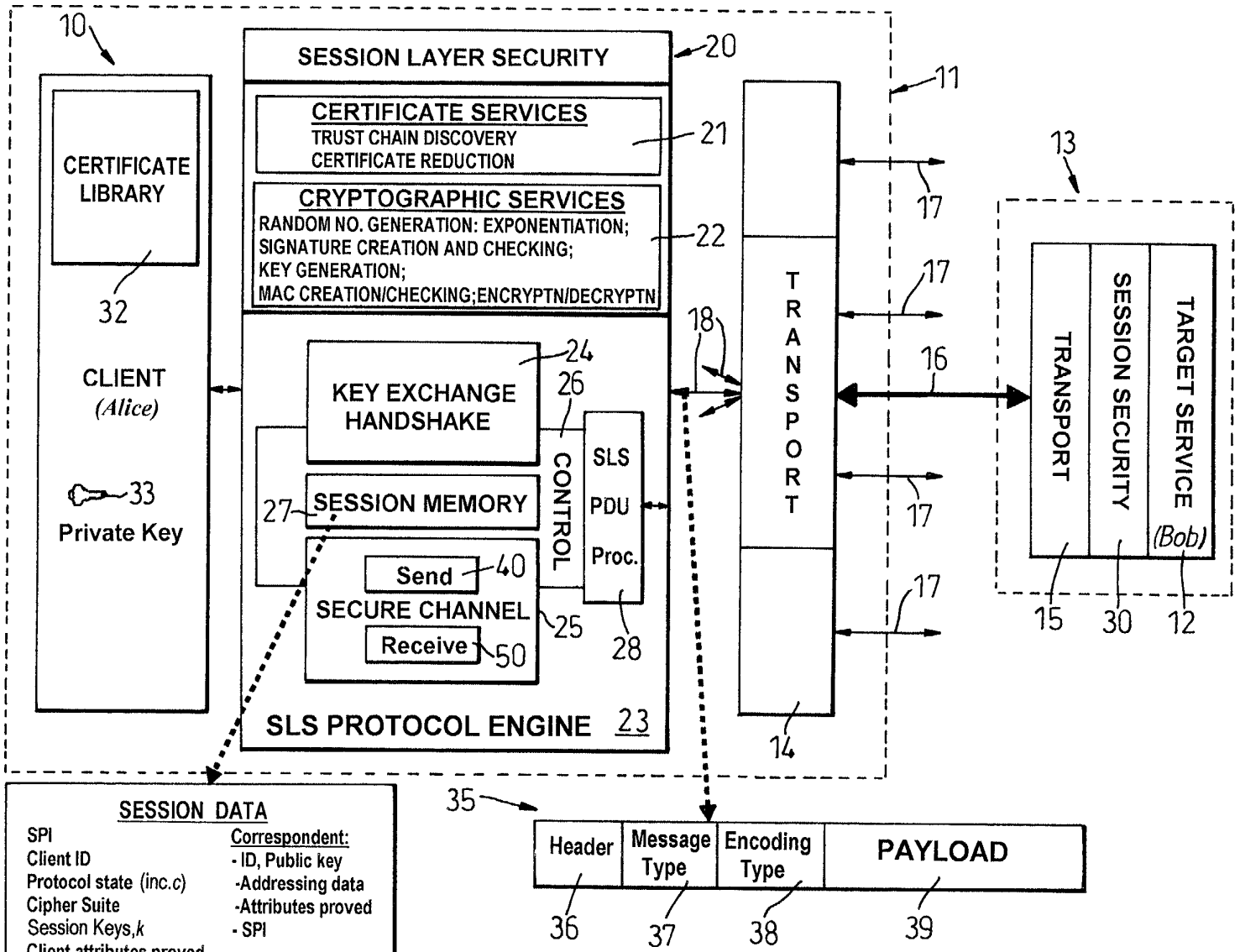
10
SESSION LAYER SECURITY
20
CERTIFICATE SERVICES
TRUST CHAIN DISCOVERY
CERTIFICATE REDUCTION
21
CRYPTOGRAPHIC SERVICES
RANDOM NO. GENERATION: EXPONENTIATION;
SIGNATURE CREATION AND CHECKING;
KEY GENERATION;
MAC CREATION/CHECKING;ENCRYPTN/DECRYPTN
22
CERTIFICATE LIBRARY
32
CLIENT
(Alice)
33
Private Key
KEY EXCHANGE HANDSHAKE
24
26
SESSION MEMORY
27
CONTROL
SLS PDU Proc.
Send
40
SECURE CHANNEL
Receive
50
25
28
SLS PROTOCOL ENGINE
23
18
TRANSPORT
11
14
17
16
13
TRANSPORT
SESSION SECURITY
TARGET SERVICE
(Bob)
15
30
12
SESSION DATA
SPI
Client ID
Protocol state (inc.c)
Cipher Suite
Session Keys,k
Client attributes proved
Nested Session SPI (if any)
Correspondent:
- ID, Public key
-Addressing data
-Attributes proved
- SPI
29
35
Header
Message Type
Encoding Type
PAYLOAD
36
37
38
39

Fig. 1

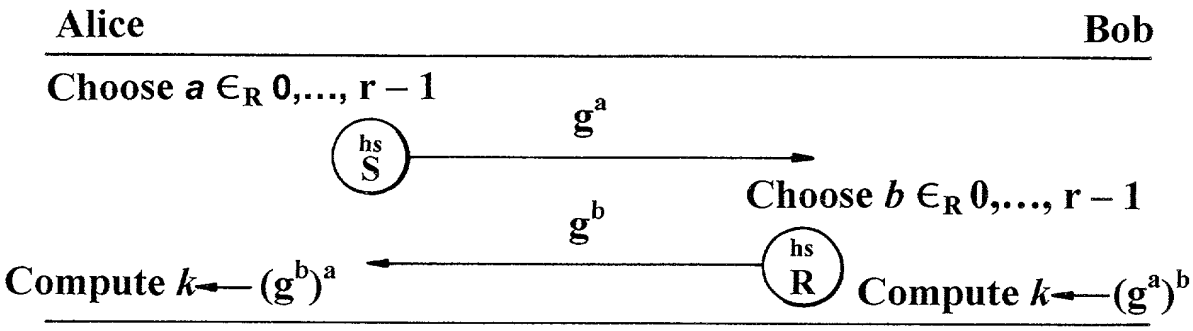
Alice
Bob
Choose $a \in_R 0,\ldots, r-1$
hs S
g^a
Choose $b \in_R 0,\ldots, r-1$
g^b
hs R
Compute $k \leftarrow (g^b)^a$
Compute $k \leftarrow (g^a)^b$

Fig. 2

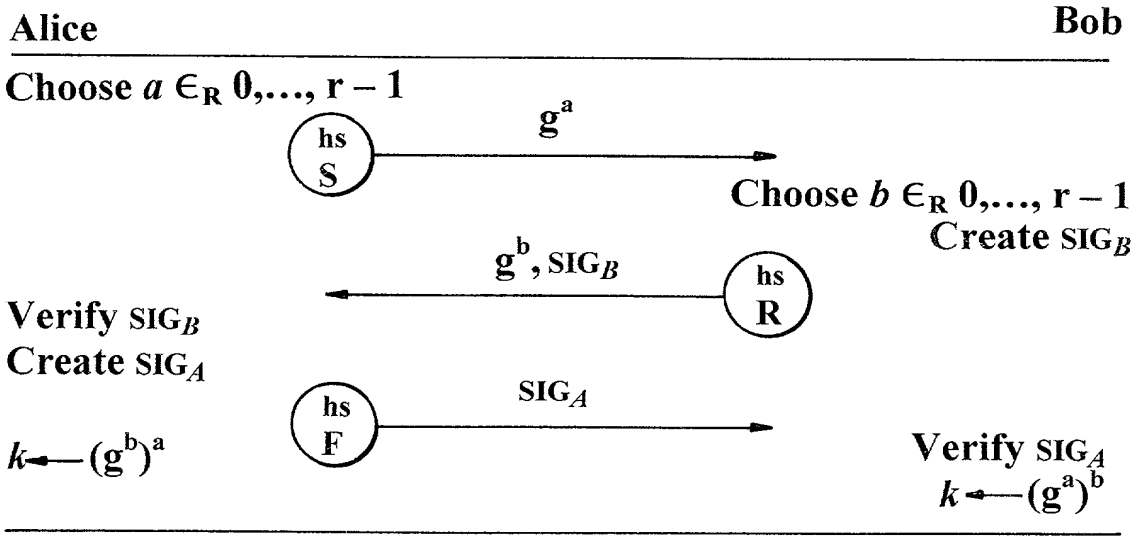
Alice
Bob
Choose $a \in_R 0,\ldots, r-1$
hs S
g^a
Choose $b \in_R 0,\ldots, r-1$
Create SIG_B
g^b, SIG_B
hs R
Verify SIG_B
Create SIG_A
hs F
SIG_A
$k \leftarrow (g^b)^a$
Verify SIG_A
$k \leftarrow (g^a)^b$

Fig. 3

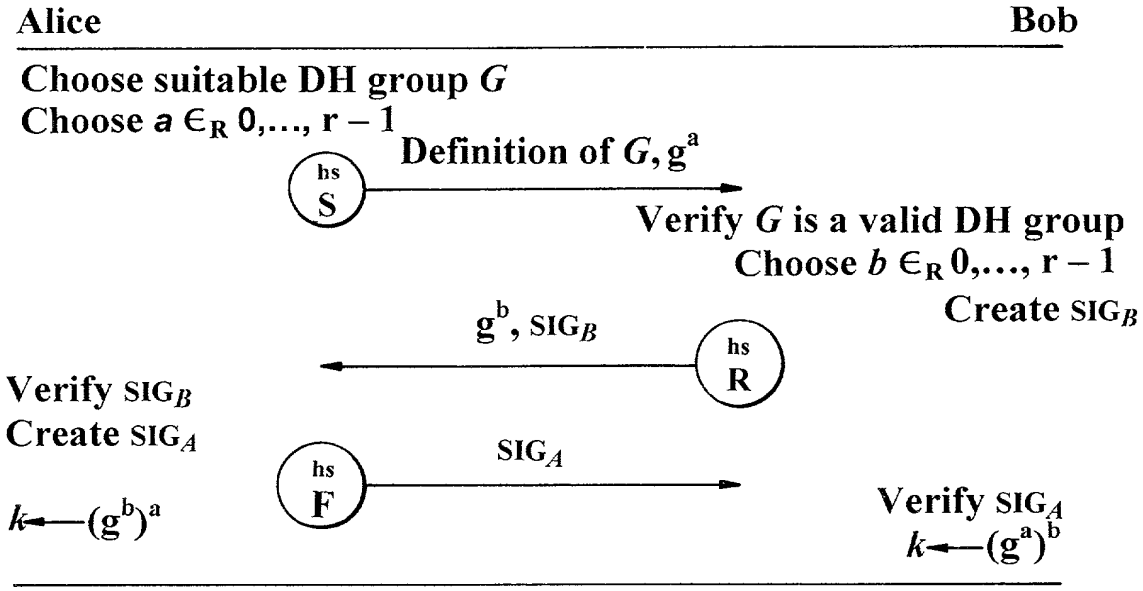
Alice
Bob
Choose suitable DH group G
Choose a ∈R 0,..., r – 1
Definition of G, g^a
hs S
Verify G is a valid DH group
Choose b ∈R 0,..., r – 1
Create SIGB
g^b, SIGB
hs R
Verify SIGB
Create SIGA
SIGA
hs F
k←(g^b)^a
Verify SIGA
k←(g^a)^b

Fig. 4

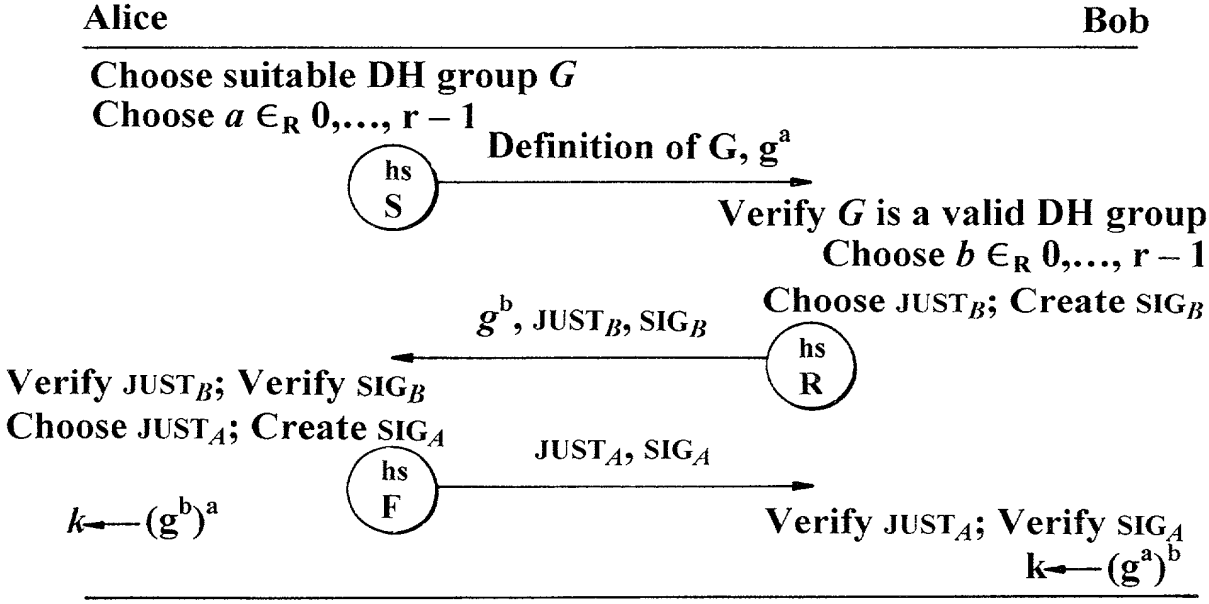
Alice
Bob
Choose suitable DH group G
Choose a ∈R 0,..., r – 1
Definition of G, g^a
hs S
Verify G is a valid DH group
Choose b ∈R 0,..., r – 1
Choose JUSTB; Create SIGB
g^b, JUSTB, SIGB
hs R
Verify JUSTB; Verify SIGB
Choose JUSTA; Create SIGA
JUSTA, SIGA
hs F
k←(g^b)^a
Verify JUSTA; Verify SIGA
k←(g^a)^b

Fig. 5

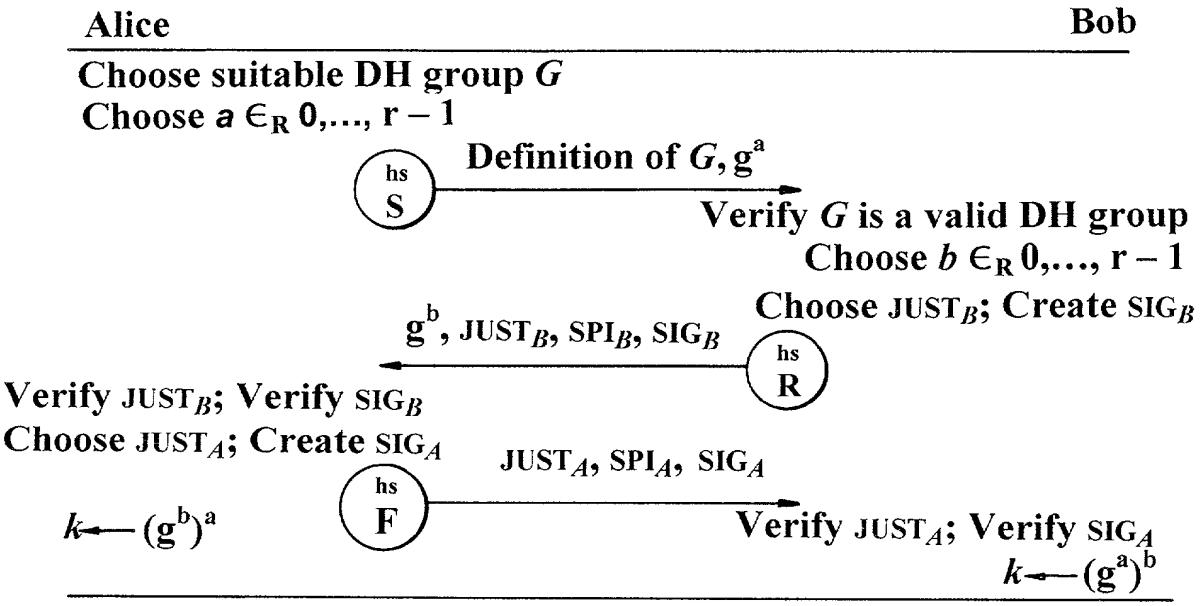
Alice
Bob
Choose suitable DH group G
Choose a ∈R 0,..., r – 1
hs S
Definition of G, g^a
Verify G is a valid DH group
Choose b ∈R 0,..., r – 1
Choose JUST_B; Create SIG_B
g^b, JUST_B, SPI_B, SIG_B
hs R
Verify JUST_B; Verify SIG_B
Choose JUST_A; Create SIG_A
JUST_A, SPI_A, SIG_A
hs F
k ← (g^b)^a
Verify JUST_A; Verify SIG_A
k ← (g^a)^b

Fig. 6

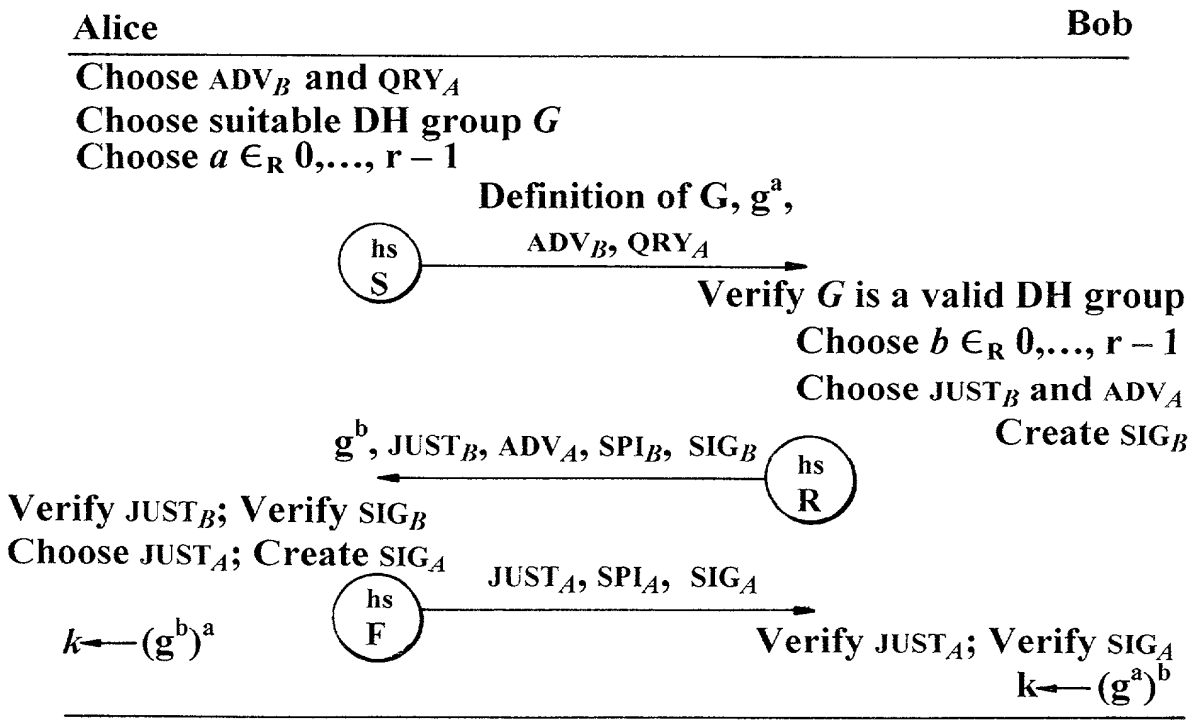
Alice
Bob
Choose ADV_B and QRY_A
Choose suitable DH group G
Choose a ∈R 0,..., r – 1
Definition of G, g^a,
hs S
ADV_B, QRY_A
Verify G is a valid DH group
Choose b ∈R 0,..., r – 1
Choose JUST_B and ADV_A
Create SIG_B
g^b, JUST_B, ADV_A, SPI_B, SIG_B
hs R
Verify JUST_B; Verify SIG_B
Choose JUST_A; Create SIG_A
JUST_A, SPI_A, SIG_A
hs F
k ← (g^b)^a
Verify JUST_A; Verify SIG_A
k ← (g^a)^b

Fig. 7

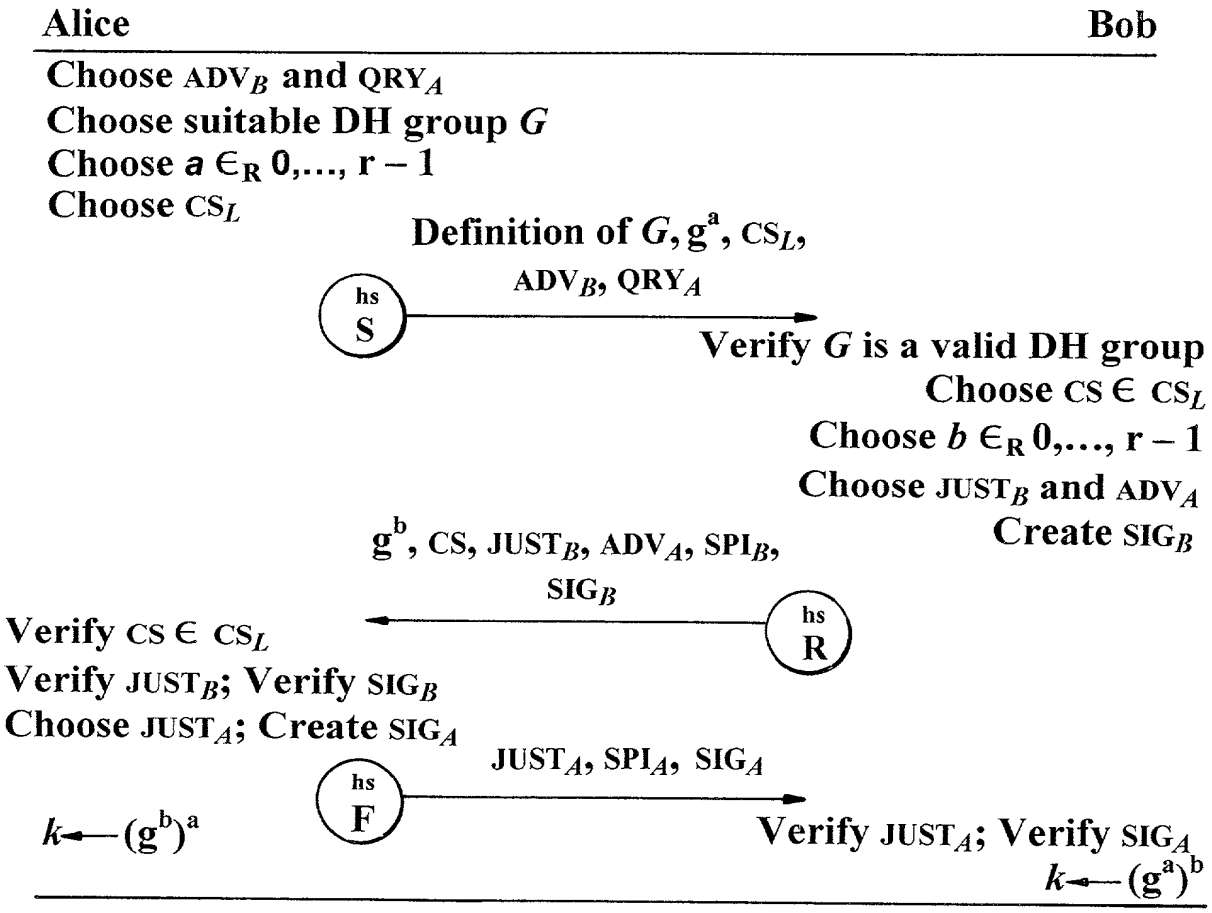
Alice
Bob
Choose ADV$_B$ and QRY$_A$
Choose suitable DH group G
Choose $a \in_R 0,\ldots, r-1$
Choose CS$_L$
Definition of G, g^a, CS$_L$,
ADV$_B$, QRY$_A$
hs
S
Verify G is a valid DH group
Choose CS $\in$ CS$_L$
Choose $b \in_R 0,\ldots, r-1$
Choose JUST$_B$ and ADV$_A$
Create SIG$_B$
g^b, CS, JUST$_B$, ADV$_A$, SPI$_B$,
SIG$_B$
hs
R
Verify CS $\in$ CS$_L$
Verify JUST$_B$; Verify SIG$_B$
Choose JUST$_A$; Create SIG$_A$
JUST$_A$, SPI$_A$, SIG$_A$
hs
F
$k \leftarrow (g^b)^a$
Verify JUST$_A$; Verify SIG$_A$
$k \leftarrow (g^a)^b$

Fig. 8

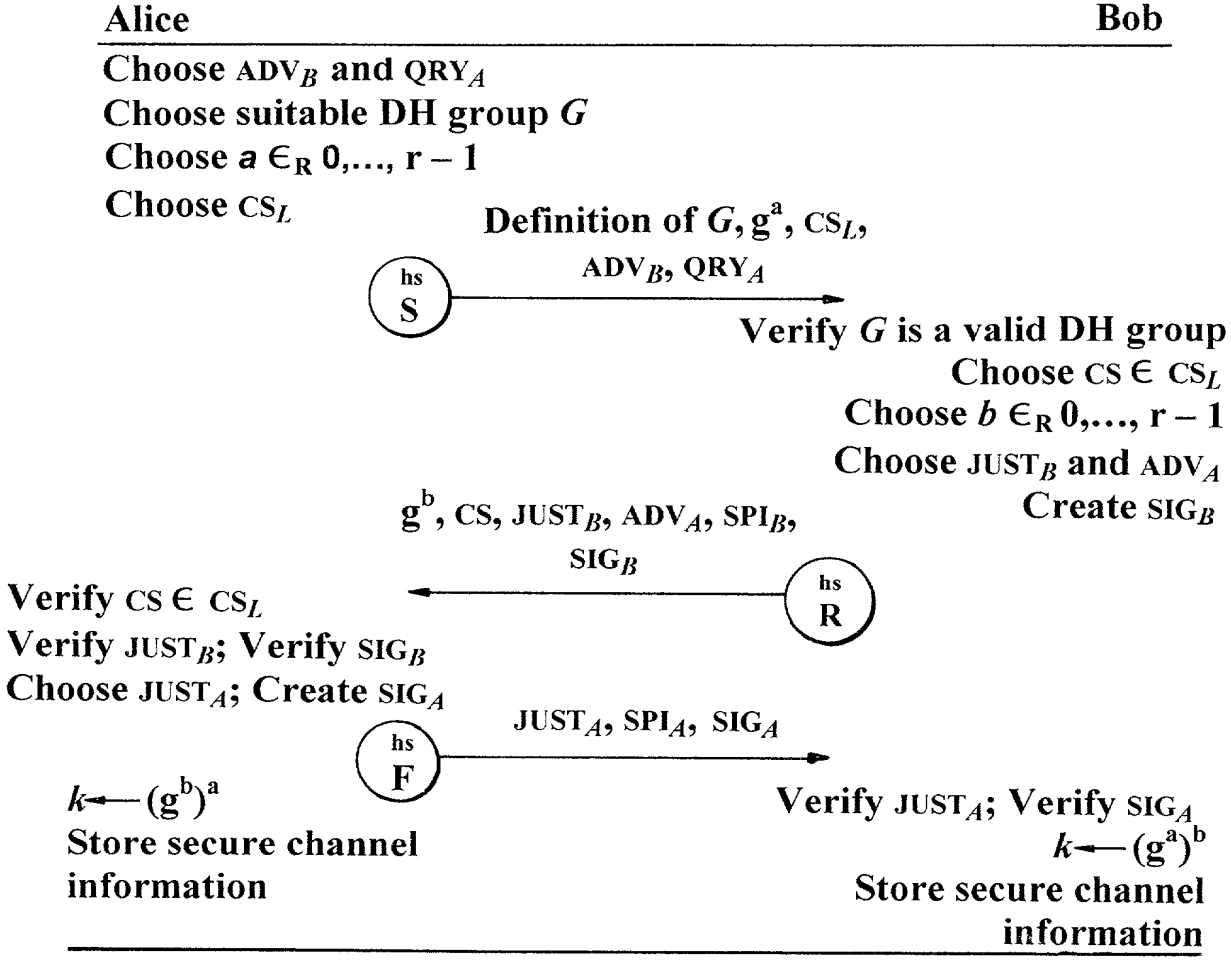
Alice
Bob
Choose ADV$_B$ and QRY$_A$
Choose suitable DH group G
Choose $a \in_R 0,\ldots, r-1$
Choose CS$_L$
Definition of G, g^a, CS$_L$, ADV$_B$, QRY$_A$
hs S
Verify G is a valid DH group
Choose CS $\in$ CS$_L$
Choose $b \in_R 0,\ldots, r-1$
Choose JUST$_B$ and ADV$_A$
Create SIG$_B$
g^b, CS, JUST$_B$, ADV$_A$, SPI$_B$, SIG$_B$
hs R
Verify CS $\in$ CS$_L$
Verify JUST$_B$; Verify SIG$_B$
Choose JUST$_A$; Create SIG$_A$
JUST$_A$, SPI$_A$, SIG$_A$
hs F
$k \leftarrow (g^b)^a$
Store secure channel information
Verify JUST$_A$; Verify SIG$_A$
$k \leftarrow (g^a)^b$
Store secure channel information

Fig. 9

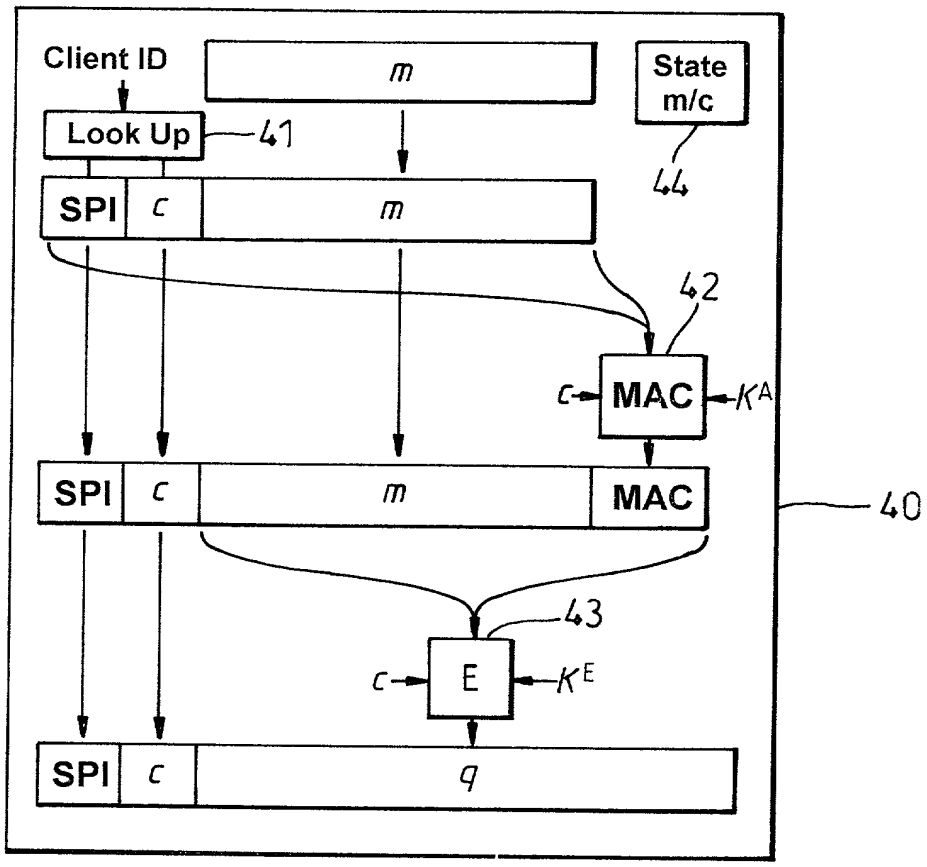
Client ID
m
State m/c
Look Up
41
44
SPI
c
m
42
c
MAC
K^A
SPI
c
m
MAC
40
43
c
E
K^E
SPI
c
q

Fig. 10

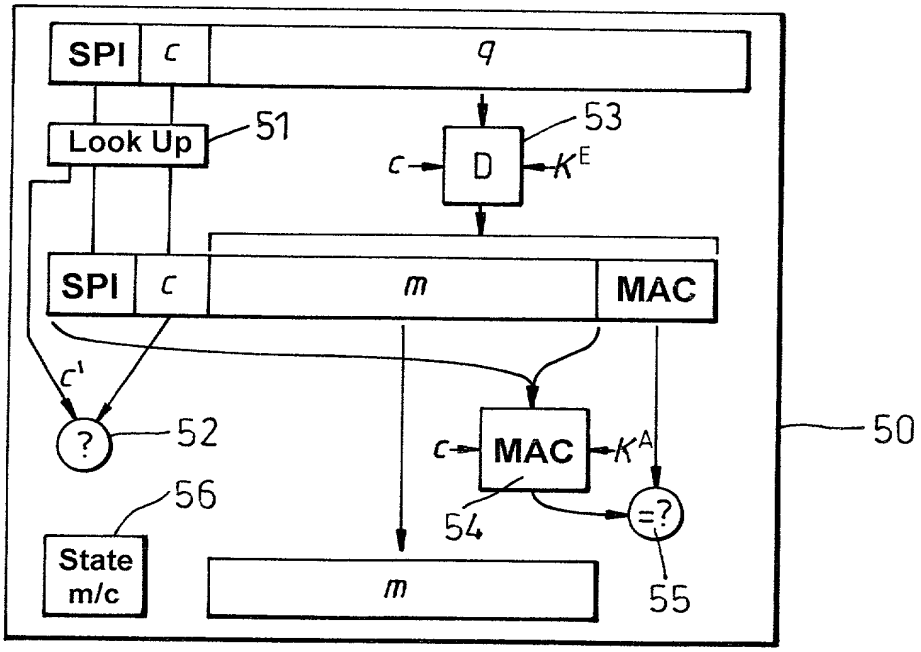
SPI
c
q
Look Up
51
53
c
D
K^E
SPI
c
m
MAC
c'
?
52
c
MAC
K^A
50
56
54
=?
State m/c
m
55

Fig. 11

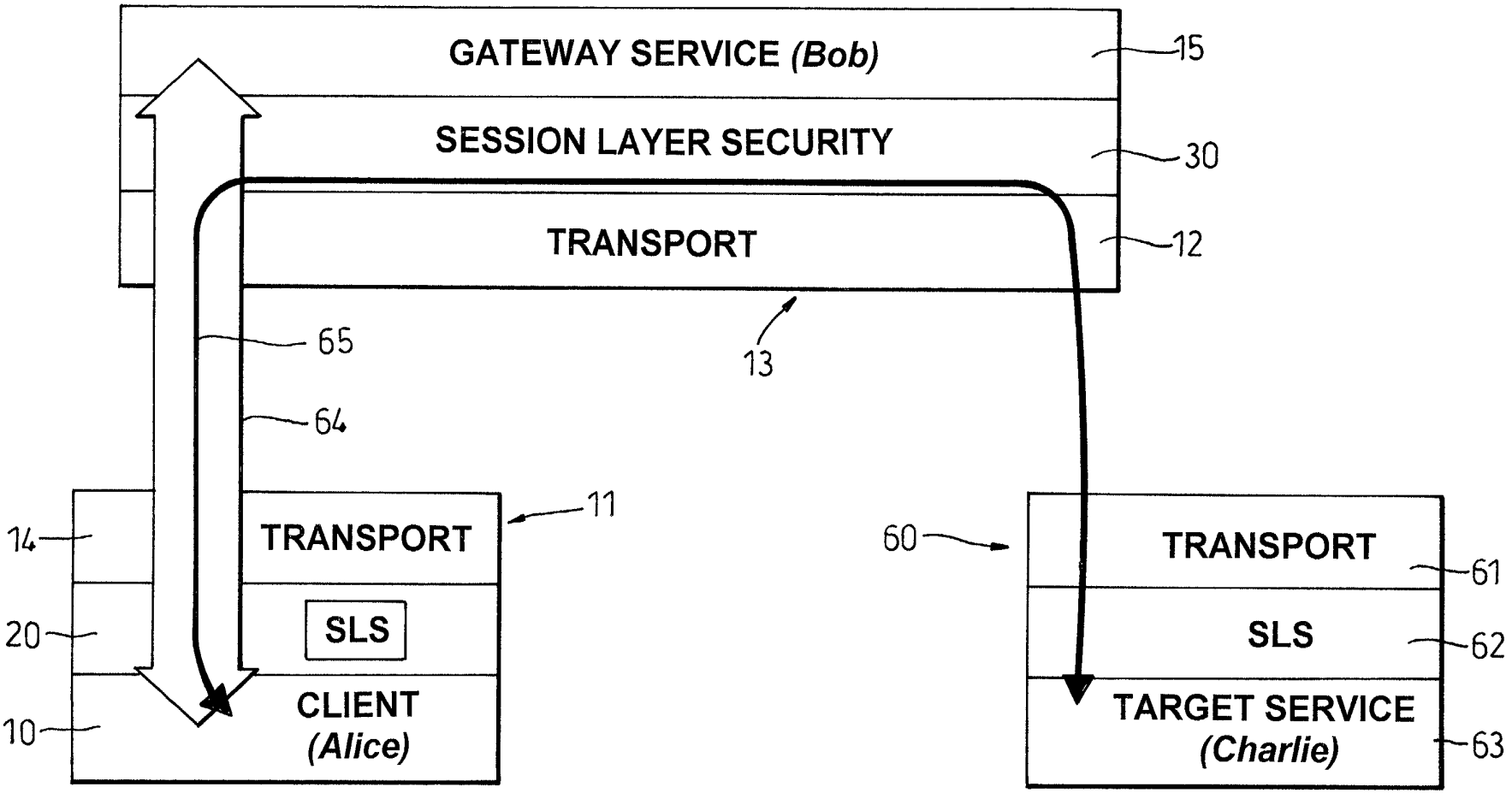
GATEWAY SERVICE (Bob)
15
SESSION LAYER SECURITY
30
TRANSPORT
12
13
65
64
14
TRANSPORT
11
20
SLS
10
CLIENT
(Alice)
60
TRANSPORT
61
SLS
62
TARGET SERVICE
(Charlie)
63

Fig. 12

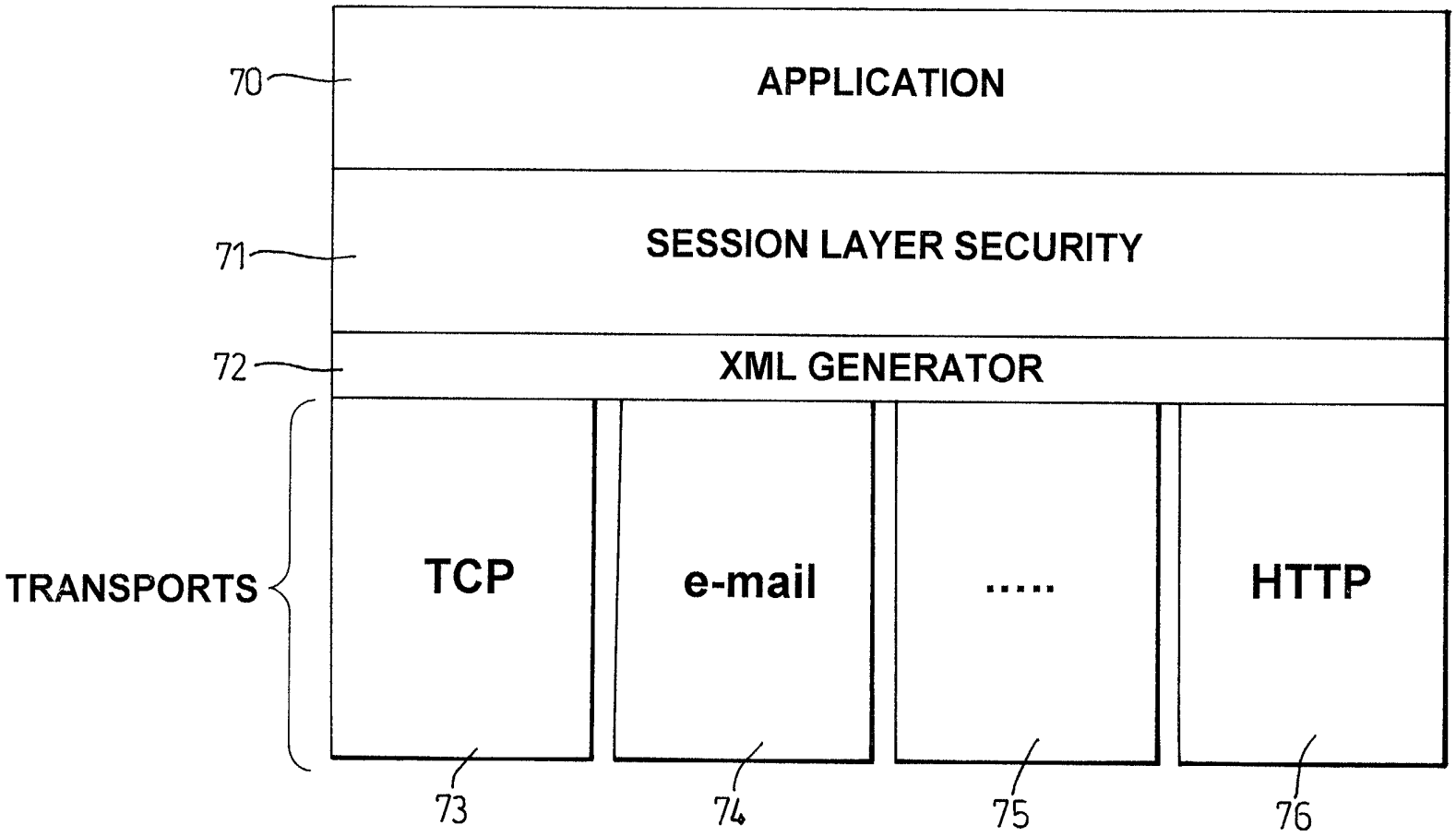

Fig. 13

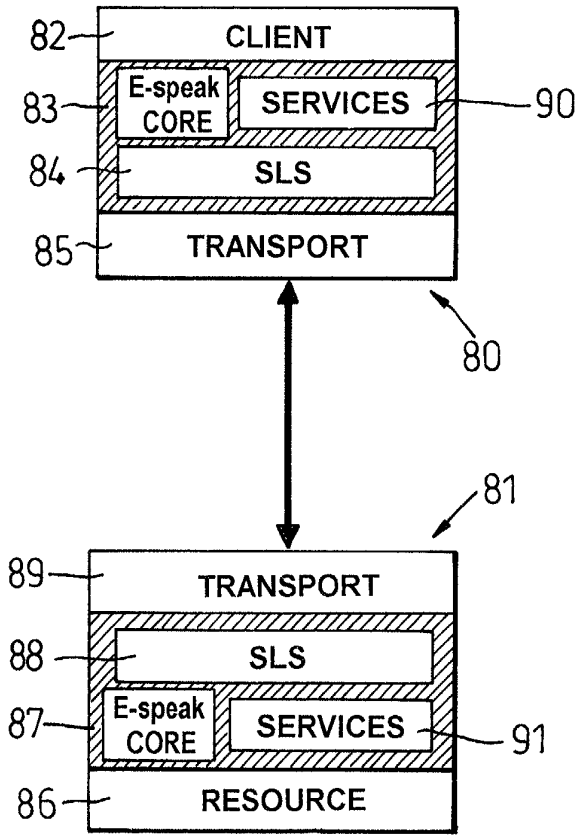

Fig. 14

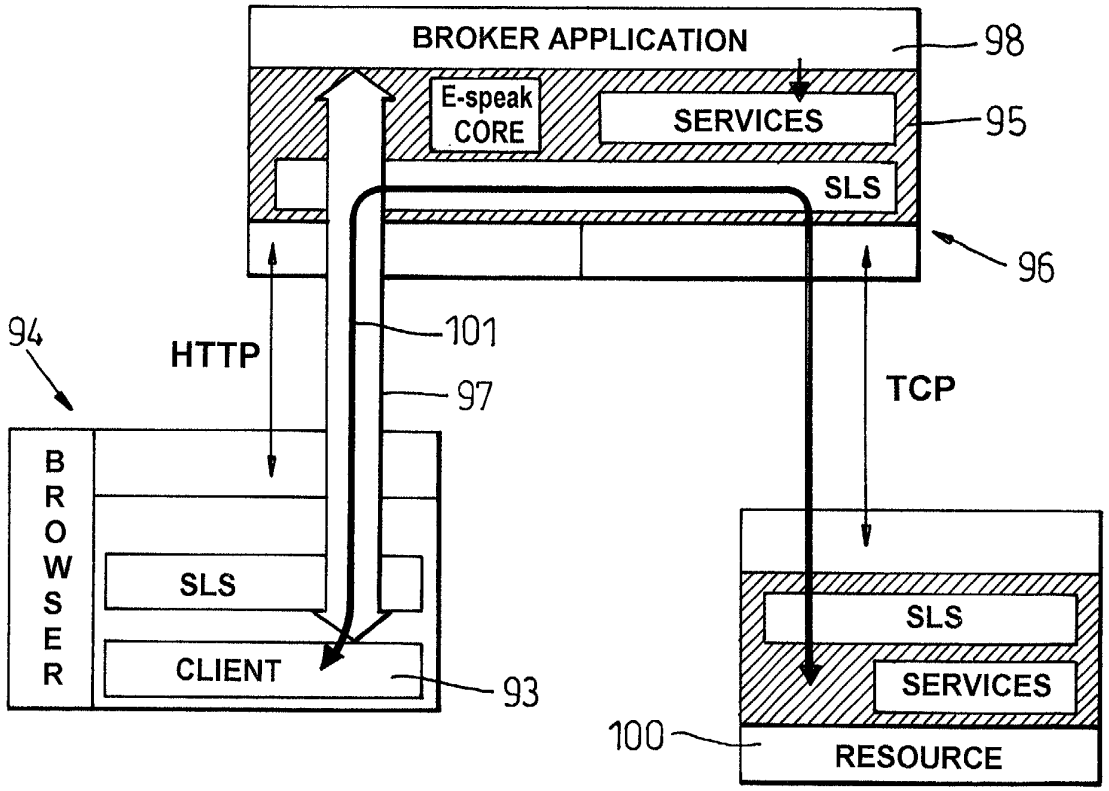

Fig. 15

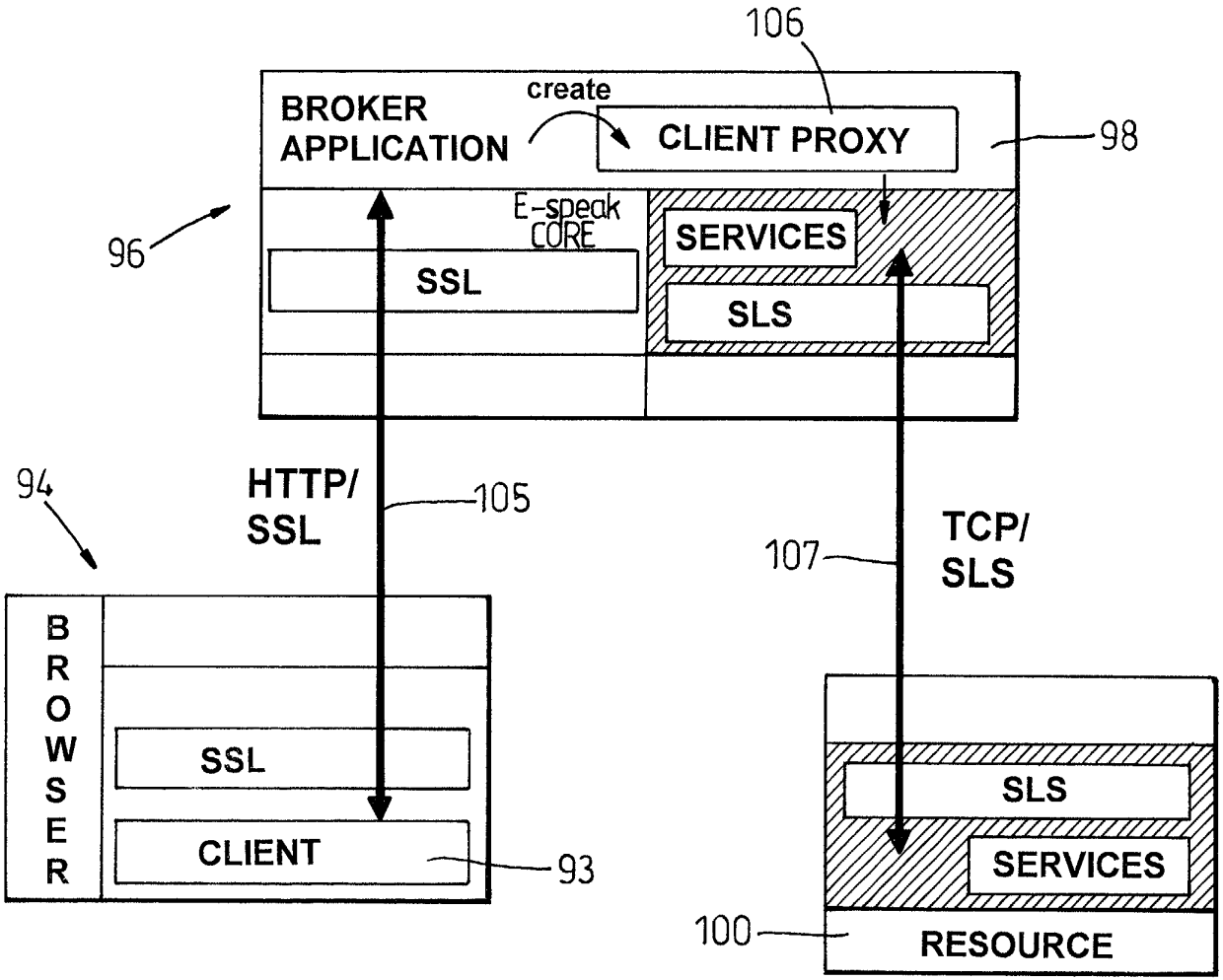
106
BROKER APPLICATION
create
CLIENT PROXY
98
E-speak CORE
SERVICES
SLS
SSL
96
94
HTTP/ SSL
105
107
TCP/ SLS
BROWSER
SSL
CLIENT
93
SLS
SERVICES
100
RESOURCE

Fig. 16